Table of Contents

1.0 Introduction

The Pegasus Design Safety Requirements Document was prepared by the Orbital Sciences Corporation (OSC) System Safety Manager to establish minimum design, test, and data requirements for the Pegasus launch vehicle and payloads. These requirements are intended to protect personnel during ground processing, and to protect the carrier aircraft and its crew. Requirements in this document apply to all flight hardware and related airborne support equipment (ASE) . Detailed requirements for ground support equipment (GSE) and ground operations safety are documented in TD-0018, Pegasus Safety Requirements for Ground Operations.

1.1 General Safety Standards

The safety design standards documented herein generally meet or exceed the minimum requirements established in government standards including ESMC and WSMC 127-1 and GHB 1771.1. These documents take precedence when operating on the respective ranges.

1.2 Safety Documentation

Safety data and results of analyses specified in this document shall be documented in a Safety Data Package (SDP) or Accident Risk Assessment Report (ARAR). The format and contents of these documents should follow the guidelines set forth in Appendix A

1.3 Control of Hazards

The following preference from MIL-STD-882 is given for the control of hazards:

a) Design for Minimum Hazard - Selection of appropriate design features to promote damage control, containment and isolation of potential hazards.

b) Safety Devices - Devices implemented to minimize a hazard or reduce the risk to acceptable levels where hazards cannot be eliminated or controlled through inherent design features.

c) Warning Devices - Employed for the timely detection of a hazardous condition and coupled with emergency controls or corrective action.

d) Special Procedures - Developed to counter potentially hazardous conditions for the enhancement of safety when inherent design features or controls are not adequate for reducing risk to acceptable levels.

1.4 General Safety Requirements

The design and operation of the Pegasus system, including payload, must satisfy the safety requirements specified in this document to ensure safety is achieved during all phases of ground processing and captive flight operations up to Pegasus achieving a safe distance from the carrier aircraft. Hazard control is accomplished through design

margin, compliance with design standards or incorporation of inhibits. In general the following requirements shall be complied with:

a) No combination of two failures or operator error shall result in either: 1) catastrophic damage to ground facilities or carrier aircraft, or 2) crew death. Catastrophic damage to carrier aircraft or ground facility is considered to be sufficient damage that results in total loss of flight worthiness of the carrier aircraft or a major facility damage. Release of Pegasus to protect the carrier aircraft or its crew is not an acceptable design hazard control.

b) No single failure or operator error shall result in significant personnel injury or damage to the flight hardware.

c) Capability shall exist to remove power from Pegasus and its payload in the event of losing safety critical inhibits during captive flight.

d) GSE and ASE interfacing with flight hardware shall be designed to be fail-safe.

1.5 Hazard Analyses

The design of flight hardware and support equipment provides the principle means of hazard control and is thus subject to safety analyses. Several analytical techniques may be employed to confirm the control of hazards and the adequacy of safety related design features. Throughout the design processes potential hazards should be progressively identified and evaluated using these analyses.

The following analyses shall be performed, by the responsible contractor, to identify hazards and the associated design and/or operational controls implemented to reduce associated risk to acceptable levels. Existing analyses may be used to the maximum extent possible.

a) Preliminary Hazard Analysis - A Preliminary Hazard Analysis (PHA) shall be performed to obtain an initial evaluation of the potential hazards for new hardware subsystems. The PHA will be started early in the design so that recommended hazard controls may be considered in the design. The PHA shall address hazardous components, environmental constraints, procedures, support equipment, and safety-related equipment.

   The PHA format identifies the hazard, the mission phase in which the hazard may be encountered (ie, ground processing, captive flight, boost) the hazard causes, any applicable safety requirements, the severity of the uncontrolled hazard consequences, and the probability of experiencing an uncontrolled hazard.

b) System Hazard Analysis - A System Hazard Analysis (SHA) shall be performed to identify specific hazards, all credible causes, methods of control and verification. Design and operational hazard controls identified in the SHA shall relate to specified safety design requirement. The SHA may be documented on a contractor specified SHA format included with the SDP/ARAR, or in the form of a hazard report.

c) Operating Hazard Analysis - The Operating Hazard Analysis (OHA) shall be used as an aid in preparation of field processing procedures. The principles of the OHA will be based on applicable field site safety requirements and correlated with the System Hazard Analysis to ensure that the design is consistent to eliminate and control hazards during field processing.

OSC and the appropriate payload system safety engineers shall coordinate applicable hazard analysis with the responsible engineering activity to ensure the incorporation of safety requirements into the design or operation. Elimination/control of hazards is resolved jointly by system safety and the responsible engineering activity.

1.6 Risk Management/Safety Assessment

Hazards identified by formalized hazard analyses are categorized in terms of criticality and probability of occurrence. Definitions for hazard severity and probability of occurrence are documented in Table 1-1 and Table 1-2 respectively.

A Hazard Action Matrix, shown in Figure 1-1, is used to determine what action is required to correct or accept each identified hazard. Full compliance with the requirements stated in this document assures that the probability of a potential hazard is reduced to the acceptable level.

To assure that controls identified for each hazard are implemented, hazard tracking shall be accomplished through a hazard control verification log which summarizes all identified hazards and highlights those that are not formally closed.

1.7 Noncompliances

OSC strongly believes that compliance with these safety requirements significantly reduces the risk to our employees of injury/death or loss of high value equipment during the integration, test and operation of the Pegasus launch system.

Noncompliance with the requirements in this document shall be listed in the SDP/ARAR. Noncompliances which are associated with an increase in the probability of a potentially critical or catastrophic hazard (e.g. reduced fault tolerance or design margin) shall be explained in detail for safety review and approval.

Residual risks from unmitigated hazards are subject to formal written acceptance by OSC, Applicable Government Agency and launch vehicle/payload program offices.

1.8 Safety Review Process (Pegasus Payloads)

1.8.1 Initial safety review (Pre-PDR)

This is an OSC safety engineering briefing to payload contractor management, engineers and designers. This meeting is intended to help the payload organization properly implement contractually imposed safety requirements, the requirements in

Table 1-1
Hazard Severity Classifications

Description	Category	Mishap Definition
Catastrophic	1	Death, system loss
Critical	2	Severe injury, severe occupational illness,or major system damage.
Marginal	3	Minor injury, minor occupational illness, or minor system damage.
Negligible	4	Less than minor injury, occupational illness, or system damage.

Figure 1-1
Hazard Action Matrix

Frequency of Occurrence	Hazard Categories Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
(A) Frequent	1A	2A	3A	4A
(B) Occasional	1B	2B	3B	4B
(C) Unlikely	1C	2C	3C	4C
(D) Remote	1D	2D	3D	4D
(E) Improbable	1E	2E	3E	4E

Hazard Risk Index	Risk Accept Criteria
1A,1B,1C,2A, 2B, 3A	Unacceptable
1D, 2C, 3B	Undesirable (Management Decision Required)
1E, 2D, 2E, 3C, 3D, 4A, 4B	Acceptable with Review
3E, 4C, 4D, 4E	Accepatable without Review

Table 1-2

Failure Probability Definitions

Description	Range	Definition
(A) Frequent	10^{-2} to 10^{-3}	A high probability of occurrence during the item operating time interval. Human error resulting from inappropriate design, maintenance manuals, or training
(B) Occasional	10^{-3} to 10^{-4}	A moderate probability of occurrence during the item operating time interval.
(C) Unlikely	10^{-4} to 10^{-5}	An unlikely probability of occurrence during the operating time interval. Zero fault tolerant design. Example undesired event caused by single failure resulting from hardware reliability or human error.
(D) Remote	10^{-5} to 10^{-6}	A remote probability of occurrence during the item operating time interval. Single fault tolerant design. Structural design factor greater than 1.0 but less than 1.5. Tailored design standard compliance. Example Any combination of two hardware failures and/or human errors resulting in undesired event.
(E) Improbable	10^{-6} to 10^{-7}	A failure whose probability of occurrence is essentially zero during the item operating time interval. Two fault tolerant design. Structural design factor greater than 1.5. Compliant with MIL-STD-1522A. Compliant with MIL-STD-1512/-1576. Example Any combination of three hardware failures and/or human errors resulting in undesired event.

this document, interpret hazard management requirements, and provide insight into previously approved hazard controls and verification methods:

a) Review conceptual payload design and potentially hazardous subsystems.

b) Verify applicable safety design criteria/hazard control methodology.

c) Identify required safety data, analyses and reporting format.

1.8.2 Preliminary Safety Assessment (PDR + 30 Days)

The purpose of the review is to present the initial results of the contractors safety analyses showing compliance with OSC safety standards:

a) Present detailed hazard subsystem descriptions

b) Identify hazard controls

c) Present preliminary safety data

d) Present preliminary results of hazard analyses.

1.8.3 Critical Safety Assessment (CDR + 30 days)

The purpose of the review is to present the detailed results of the contractors safety analyses showing compliance with OSC safety standards:

a) Present detailed hazard subsystem descriptions

b) Identify hazard controls, safeties and methods of verification

c) Present detailed safety data

d) Present results of hazard analyses.

e) Review payload ground operation requirements from safety view-point.

f) Identify hazardous operations and eliminate conflicts in integration flow.

g) Verify GSE safety requirements and hazardous procedural controls.

h) Assist in the closure of any payload safety action items.

i) Develop contingency procedure

1.8.4 Pegasus/Payload Airworthiness Review (L- 2 Months)

The purpose of the review is to present the final results of the contractors safety analyses showing compliance with OSC safety standards:

a) Formal certification for flight.

b) Close-out all Pegasus/Payload safety action items.

2.0 Overview of Facility (VAB) Safety Features

This section provides a brief overview of the primary facility safety features and procedures to follow when conducting hazardous operations within the VAB. Detailed safety requirements can be found in the Pegasus Safety Requirement Document for Ground Operation,s OSC/SSD TD-0018.

2.1 Explosive Safety Standards

The VAB is designed and operated in accordance with the regulations for explosive quantity distance siting in accordance with AFR 127-100 or DOD 6055.9-STD and for liquid propellant servicing in accordance with OSC TD-0018.

2.2 Fire-Protection

The VAB fire protection system is provided in accordance with local fire protection regulations.

2.3 Static Grounding System

A ground system check for lightning, electrical fault, and static build-up protection is provided. A floor plan type layout which shows all grounding systems test points has been developed.

2.4 Warning Signals

The VAB is required to have warning devices that alert personnel entering the area as to the status within the building. These devices consist of warning lights or audible signals. The safety related VAB warning light are defined as follows:

a. Flashing Green Light - Facility is open for normal operations.

b. Flashing Amber Light - Activated just prior to commencing hazardous operations. Do Not enter VAB without permission from the control authority, reference VAB Entry Control Procedure.

c. Flashing Red Light/Klaxon - Hazardous atmosphere. Evacuate area to greater than 100 ft.

d. Bell - Fire Alarm. Evacuate area to greater than 600 ft.

2.5 Hazardous Operations

When an operation could cause damage to equipment, injury to personnel, or degradation of system functions appropriate warning/caution devices, procedural control and/or protective equipment as defined in this document shall be implemented.

The following requirements are applicable to the performing hazardous operations:

a. Utilization of the two man rule for entry into the VAB when a complete Pegasus vehicle or individual rocket motors are present and during the accomplishment of any critical or hazardous operation.

b. Utilization of the "Reader Worker" routine during the accomplishment of any critical or hazardous operation.

c. Verification and strict adherence to procedures is required. All hazardous procedures must be reviewed and signed by the OSC Pegasus Safety Engineer and/or applicable local authorized safety personnel.

d. Briefings must be held prior to commencement of hazardous operations.

e. Coordination of hazardous operations scheduling with local authorized personnel.

3.0 Detailed Safety Related Design Requirements

This section contains the detailed safety requirements for the Pegasus flight vehicle, Payloads and associated ground support equipment. Safety data and results of testing specified in these requirements shall be documented in a Safety Data Package (SDP) or Accident Risk Assessment Report (ARAR).

3.1 Hazardous Material

A hazardous material may consist of liquids (including cleaning agents) or gases (including inert gases). It also may consist of hazardous solids that may be toxic or flammable, for example, biological, biological experiments. Materials which are not hazardous in themselves but can be hazardous in conjunction with a hazardous material, are discussed in this section and should be addressed.

3.1.1 Hazardous Material Selection

The selection of materials shall be based on consideration of the following:

a. FLAMMABILITY/COMBUSTIBILITY- Where feasible use a less flammable liquid or material where feasible and use materials such as thermal blanket, wire insulation or contamination cover which upon ignition will not burn readily.

b. TOXICITY-Use a less toxic liquid or material where feasible. Use a thermal blanket, wire insulation or contamination cover which will not give off a toxic gas if ignited, where feasible.

c. COMPATIBILITY-Use a liquid or material which is compatible with the vessel/plumbing which contains it. Do not allow the liquid to be capable of leaking at credible leak points upon a non-compatible or absorbent material, for example, thermal blanket, wire insulation or contamination cover, where feasible.

d. ELECTROSTATIC BUILD-UP -- Use of static charge generating materials shall be strictly limited. As a minimum materials shall not retain a static charge sufficient to present an ignition source to ordnance or flammable vapors.

e. EXPLOSIVE NATURE-Use a material which is not explosive in itself or in conjunction with other materials unless the explosive nature is necessary for system functioning, for example, EEDs.

3.1.2 Hazardous Material Data Requirements

The Material Safety Data Sheet (MSDS) and following data is required for hazardous materials:

a. A listing of all hazardous materials and liquids on the flight system and used in ground processing.

b. Description of how each of these materials/liquids is used and in what quantity.

c. Description of flammability and, if applicable, explosive characteristics.

d. Description of toxicity. (Provide Threshold Limit Value and other exposure limits, if available.)

e. Description compatibility. List all materials which may come in contact with a hazardous liquid/vapor. Items of concern include gaskets in propellant system and contamination covers/thermal blankets.

f. Description of electrostatic build-up on materials such as contamination covers and thermal blankets and how EEDs and propellants are exposed/protected from the discharge.

g. Description of personal protective equipment to be used with the hazardous material/liquid and other safety precautions.

h. Description of decontamination, neutralization and disposal procedures.

i. For hazardous material/liquid aboard a flight system:

   (1) A sketch showing location.

   (2) Description of protection against rupture/leaks.

   (3) Description of protection against inadvertent release of material/liquid. For propellant/pressure systems, reference where the data can be found.

3.2 Structural and Mechanical Subsystems

The safety critical characteristic for structural elements (i.e., strength) is mainly associated with applied load/temperature exceeding design strength, propagation of crack like flaws, stress corrosion and hydrogen embrittlement.

a. To reduce the probability of failure due to applied load exceeding design strength the structural members shall be designed with the factors listed in Table 1.

b. The materials selected for use in structural and mechanical designs shall be rated for resistance to stress corrosion cracking (SCC) in accordance with the tables in MSFC-HDBK-527/JSC 09604 and MSFC-SPEC-522. Alloys with high resistance to stress corrosion shall be used wherever possible and do not require OSC safety approval. When failure of a part made from low or moderate resistance alloy could result in a critical or catastrophic hazard, a material usage agreement shall be submitted to OSC safety for approval

c. Structural analysis and testing shall be performed to verify that the structure assemblies are designed with the applicable safety margins.

TABLE 1 Structural Design Factors

Condition	Uncertainty Factor	Factor of Safety Design Yield	Design Ult.
Free Flight Operations:			
Quasi-Static	Aero: 1.2 Other: 1.0	1.1	1.25
Transient	See Note 1	1.1	1.25
Man Rated Operations:			
Qusi-Static	Landing: 1.4	1.25	1.5
Transient	See Note 1	1.25	1.5

Note 1: 3dB Factor Applied to Load

3.3 Liquid Propellants/Propulsion Subsystems

This section establishes the minimum design criteria and policy to be met to ensure that liquid/gas propellant/propulsion systems, used at the VAB, are safe to handle, store, transport, be present during assembly or checkout and captive flight.

3.3.1 Flight Hardware Safety Requirements

a. Design considerations contained in the AFSC Design Handbooks DH 1-6, System Safety, Chapter 3, Section 3E and Chapter 4, Section 4B, National Electric Code (NEC), and Chemical Propulsion Information Agency (CPIA) Publication 394, Volumes I and III (AFM 161-30 Vol II) and Space Propulsion Hazards Analysis (SPHAM) provide excellent guides and should be used in the design of liquid/gas propellant/propulsion systems.

b. Propellant transfer systems for fueling and defueling propulsion GSE shall be designed to ensure that no single failure can cause damage to the flight propulsion system.

c. Leakage of propellant, premature propellant system thruster (hot gas) firing and propellant decomposition due to leakage past closed valves during ground operations or captive carry flight is considered to be catastrophic.

(1) Propulsion system shall contain a minimum of three mechanically independent flow control devices in series to prevent inadvertent thruster firing. One of the three flow control devices shall isolate the propellant tank(s) from the down stream fittings and thrusters. A normally closed pyrotechnically initiated parent metal isolation valve with two fault tolerant electrical controls is preferred. Use of a pyrotechnic valve shall be considered the equivalent of two flow control valves.

(2) The isolation valve may not be opened until after separation of Pegasus from the carrier aircraft.

(3) There shall be three independent electrical inhibits that control the opening of the flow control devices. The electrical inhibits shall be arranged such that failure of one inhibit will not open more that one flow control device.

(4) At least two of the three required independent electrical inhibits shall be monitored by the LPO or ground crew.

(5) The propellant system shall be two failure tolerant to propellant leakage past seals, seats, etc.. If the potential leak source is in a mechanically isolated segment of the propellant plumbing, failure tolerance will depend on the type and quantity of the propellant.

d Propellant over heating is considered catastrophic. Components, e.g. solenoid valves, that are capable of heating the system to temperatures greater than the fluid compatibility level shall be two fault tolerant to a failed on condition.

e. Premature propellant system thruster (hot gas) firing and propellant decomposition due to very small amounts of propellant leakage past closed thruster valves during ground operations or captive carry flight may be reduced from catastrophic to critical if the effects are mitigated by design, or analysis and/or test show the severity can be reduced.

f. Propellant pressure monitoring is mandatory for at least 12 hours after loading and during captive flight. Propellant temperature monitoring is optional after loading and during captive flight unless a credible event could cause over temperature or repeated freeze-thaw cycles.

g. Connections in the system shall be welded or brazed.

3.3.2 Propellant/Propulsion Subsystem Test Requirements.

a. Short-term compatibility tests of all materials utilized on a propellant system shall be conducted unless the degree of compatibility has been proven. Specific tests shall be conducted for such things as stress corrosion, embrittlement, reactivity, etc.

b. All new, modified or repaired propellant systems, components, or liners shall be proof-tested prior to being used with propellant. Hydrostatic proof testing shall

be 1.25 times maximum operating pressure. New systems or components, if tested by the manufacturer, shall have test description and results certified to OSC's System Safety. Proof testing shall be performed on the assembled system unless Safety approves proof testing at only the component/sub-assembly level. Welded connections for replacement components shall be proof tested.

c. New, modified, or repaired propellant storage/transfer systems shall be validated by functional tests prior to being certified for normal operational use. Procedures for performing these tests shall be approved by Range Safety. The user shall certify in writing to OSC Safety that the system/subsystems have satisfactorily passed the required tests. These tests shall include:

(1) A leak test at maximum operating pressure with an inert gas or referee fluid.

(2) Verification of control components and systems by use of certified calibrated gauges.

(3) Verification of emergency shutdown systems and procedures.

(4) Verification of proper operation of quick disconnects.

(5) See Section 3.4.4 and 3.4.5 of this document for additional test requirements regarding pressurized systems.

d. Properties of the propellant (for example, flammability and toxicity) shall be determined. Propellants that have not had TLV's and emergency short term exposure limits defined in American Conference of Governmental Industrial Hygienists Publication titled "Threshold Limit Values for Workplace Exposures" shall be tested and the results approved by the Air Force Surgeon General or other DOD agency approval office to establish their limits.

3.3.3 Propellant/Propulsion Subsystem Data Requirements.

a. The type and chemical composition of the propellants and amount in gallons and pounds normally used in each tank of the launch vehicle or payload. Specify any test fluid or gas that will be used in the system.

b. A sketch showing the location of all tanks and lines on the launch vehicle, payload or GSE. Also differentiate between load, drain, purge, vent, pressure and sampling lines.

c. Mechanical drawings or sketches showing the physical position and a description of operation for all components and subsystems. Identify the means of shutting off propellant flow manually. Identify and describe sampling capability. Drawings should contain sufficient identification and explanatory notes.

d. Functional schematic/drawings (mechanical and electrical) of the system, with identification of components and subsystems in such a manner as to be usable with operating procedures. Drawings must be equipped with a legend. Include all mechanical inhibits electrical control circuitry. Identify all pressure levels, ranges and settings and pressure safety features

e. A list of all components and the material of which they are composed. Include soft goods, (for example, valve seats, gaskets, etc.).

f. Compatibility studies, of the propellants, test fluids or pressurizing/purging gases versus materials in the system. A statement certifying compatibility of materials shall be included.

g. Procedures for loading, detanking and flushing operations. Specify associated hardware.

h. A detailed description, with mechanical drawings or sketches, of the operation of each component with emphasis on safety features which prevent inadvertent operation. Drawings should contain sufficient identification and explanatory notes.

j. A list and synopsis of all propellant related procedures and approximate time lines. Detailed procedures on all propellant operations are required:

(1) Maximum credible spill size (volume and surface area).

(2) Description of hazards other than toxicity, for example, flammability, reactivity, etc. Identify material short-term compatibility problems in the event of a spill.

(3) Protective equipment to be used in handling and using the propellants. Be specific as to when this equipment will be used during an operation. Specify manufacturer, model number, etc.

(4) Manufacturer, model number, specifications, operating limits, type of certification and general description of vapor detecting equipment.

(5) Recommended methods and techniques for decontamination of areas affected by spills or vapor clouds and hazardous waste disposal procedures.

3.4 Pressurized Components

This section establishes the basic safety criteria for pressurized systems used on flight hardware which contain pressurized systems, subsystems or components. These systems include liquid propellants, gas or hydraulic fluids, and vacuum systems. Design considerations contained in MIL-STD-1522; ASME Boiler and Pressure Vessel Code, Section VIII, Division 1 and 2 provide excellent guides and shall be used when specifically referenced in this section. In the event of conflict between the documents referenced herein and the contents of this pressure systems section, the contents of this section shall be considered as superseding requirements. Low pressure systems are not relieved of the requirements of this section.

3.4.1 Definitions

For the purpose of this document, the following definitions are provided to ensure precision of meaning and consistency of usage.

a. FLIGHT HARDWARE- includes all propellant tanks, pressure vessels, lines and components that constitute airborne equipment on a launch vehicle or payload.

b. GROUND SUPPORT EQUIPMENT (GSE)- includes all propellant tanks, high pressure vessels, lines and components that are used to support prelaunch, launch, and post launch operations, except for compressed gas cylinders (K-bottles), mobile tankers and compressed gas trailers that must meet DOT requirements. Ground support equipment not involved in launch activity may also be covered by this section if propellants or other significant hazards are involved.

c. MAXIMUM EXPECTED OPERATING PRESSURE (MEOP)-The maximum pressure a system will be subjected to during static and dynamic conditions.

d. MAXIMUM ALLOWABLE WORKING PRESSURE (MAWP)-The maximum operating pressure permissible for a pressure vessel, tubing, piping, flex hose or component at the operating temperature specified for that pressure. It is a component's pressure rating based on structural and functional reliability.

e. PROOF PRESSURE-The test pressure applied to pressure systems or individual components without failure, leakage, or permanent deformation.

f. DESIGN BURST PRESSURE-This pressure is a test pressure that pressurized components must withstand without rupture to demonstrate its design adequacy in a qualification test.

g. EMERGENCY SYSTEM/COMPONENT-An emergency system component is any system/component which prevents a hazardous event from occurring or escalating. These systems normally experience very few cycles, but their performance is extremely safety critical. Typical emergency components are relief valves and shut-off valves. Typical emergency systems are fire suppression systems and emergency purge/vent systems.

h. PRESSURE RANGE-The pressure range covered by this manual is 0 to 15,000 psia. The upper limit is predicated by the present technological knowledge and limitations and can be expected to change in the future. Pressure system safety precautions apply to all pressures in this range. The degree of hazard in pressure systems is proportional to the amount of energy stored, not the amount of pressure present. Therefore, low-pressure, high-volume systems can be as hazardous to personnel as high-pressure systems. Pressures systems of less than 150 psi, or less than 75,000 ft. lb. output energy, may be relieved of certain requirements on a case-by-case basis, depending on hazard potential, as determined by OSC Safety.

Pressure systems shall be designated as follows:

Low Pressure	0 to 500 psi
Medium Pressure	501 to 3,000 psi
High Pressure	3,001 to 10,000 psi
Ultra High Pressure	above 10,000 psi

3.4.2 Design Requirements

a. Flight hardware propellant tanks and vessels shall be designed to one of the following sets of criteria:

(1) The ASME Boiler and Pressure Vessel Code, Section VIII, Division 1 or 2. Division 1 requires a safety factor of 4; Division 2 requires a safety factor of 3 in conjunction with extensive analysis and testing.

(2) MIL-STD-1522. This requires a minimum safety factor of ≥ 1.5:1. Depending on local requirements minimum safety factor may be 2:1 for non-leak-before-burst designs.

(3) Other standard. Vessels and tanks which are not designed IAW ASME or MIL-STD-1522 shall be approved by OSC Safety. A safety factor of 2:1 is required unless the design, fabrication and testing is consistent with the criteria of Mil-Std-1522 as determined by OSC Safety. Use of MIL-STD-1522 is recommended for all vessels/tanks. The required degree of compliance will vary with the safety factor provided.

b. All flight hardware pressure systems shall be identified as follows:

(1) Pressure vessels built to comply with the ASME Pressure Vessel Code shall be identified using ASME Pressure Vessel Code Identification requirements.

(2) All other pressure vessels shall be traceable to a log book which conspicuously specifies the following information:

- Maximum allowable working pressure (psig).
- Proof pressure (psig).
- Design Burst Pressure (psig).
- Operational cycle limits.
- Operational temperature limits (°F).

c. Tanks and vessels shall be designed for safe endurance against hazardous failure modes for not less than 400% of the total number of expected cycles.

d. As a minimum, pressurized tubing, piping, hoses and fittings for flight hardware pneumatic systems shall have a design burst pressure equal to 4.0 x maximum operating pressure.

e. Other pressure system elements not considered lines or fittings shall have a design burst pressure equal to 2.5 x maximum operating pressure.

f. No part of a pneumatic pressure system shall fail, take any permanent set, or be damaged in any manner when subjected to a proof pressure.

3.4.3 Pressure Relief and Venting Requirements

ASME Boiler and Pressure Vessel Code, Section VIII, Division 1 or 2 provides an excellent design guides for pressure relief and venting. They should be used to the extent that they do not conflict with the following requirements.

a. Pressure relief devices shall be installed on all systems having an on-board pressure source that can exceed the MAWP of any component downstream of that source unless the system is electrically and mechanically single fault tolerant against exceeding MAWP.

b. The system shall be electrically and mechanically two fault tolerant against exceeding burst pressure of any component downstream of an on-board pressure source.

c. Flight hardware pressure systems that require on-board relief capability shall comply with GSE pressure relief requirements.

d. During pre-launch pressurization of flight hardware:

1) Relief devices shall be provided on the flight hardware or GSE to protect the flight hardware (launch vehicles using GSE relief devices for protection shall remain connected to the GSE system as long as possible prior to launch)

2) Pressure monitoring capability is mandatory unless there are no credible events that could result in exceeding the MAWP of the tank,lines, fittings or components in the system.

3.4.4 Testing Pressure Components

a. Flight vessels/tanks designed in accordance with MIL-STD-1522 shall undergo qualification and proof testing in accordance with MIL-STD-1522 requirements.

b. Flight vessels/tanks not designed and built in accordance with Mil-Std-1522 shall be qualified and proof tested to levels and conditions approved by Safety. Unless otherwise approved, a hydrostatic proof test at 1.25 MAWP, a burst test and a cycle test is required. Welds shall be inspected and tested.

c. Other pressure system elements not considered lines, fittings, gauges or vessels shall be hydrostatically proof tested to 1.5 times the components' MAWP.

3.4.5 Testing Flight_Pressure Systems

a. All newly assembled pressure systems shall be hydrostatically proof tested to 1.25 x MEOP prior to normal use. Where this is not possible, OSC Safety will determine the adequacy of component proof testing and alternate means of testing and alternate means of testing the assembled system. Welds which cannot be proofed shall be X-rayed.

b. Pneumatic proof testing to a proof pressure of 1.25 x MEOP in lieu of hydrostatic testing is permissible if hydrostatic proof testing is impractical, impossible or will jeopardize the integrity of the system or system element. prior approval for pneumatic proof testing at the VAB must be obtained from OSC Safety.

c. Any pressure system or system element that has been repaired, modified or possibly damaged, subsequent to having been proof tested, shall be re-tested at proof pressure prior to its normal use. If a component is to be welded into the system, both the component and the weld must be proofed.

d. All new, modified or repaired pressure system shall be functionally tested at the system MOP prior to their normal use.

e. All new, modified or repaired pressure systems shall be leak tested with an inert medium at the system MOP prior to its normal use.

f. If any pressure system element (valve, regulator, gages, tubing, etc.) has been disconnected/reconnected for any reason, the affected system or subsystem must be revalidated with a leak test using an inert medium.

g. Pressure relief valves shall be tested for proper setting and operation prior to normal use. Relief valves shall be re-tested whenever damage is suspected, or as a minimum, once a year. The valve shall be marked accordingly.

h. Pressure gages shall be calibrated prior to normal (first) use. Pressure gages shall be re-calibrated whenever damage is suspected or as a minimum, once a year. The gage shall be marked accordingly.

3.4.6 Pressure System Data

The following information is required for all pressure system elements:

a. Identify each element with a reference designation permitting cross reference with the system schematic.

b. MAWP for all pressure system elements. Also identify the MEOP the element shall see when installed in the system.

c. Safety factors or design burst pressure for all pressure system elements. Identify actual burst pressures if available.

d. Proof pressure for each system element. Also identify the proof pressure the element will see after installation in the system.

e. Materials used in fabrication of each element, to include soft goods.

f. Cycle limits if fatigue is a factor in the system.

g. Temperature limits of each system component.

h. Design allowable/tolerances, other than temperatures and pressures which may affect component/material performance.

i. Manufacturer's name, model number and part number of all components. Indicate which components are procured per specification drawing. If a non-standard component is used, provide a cross-sectional assembly drawing of the component and any additional data required to evaluate the safety aspects of the element.

j. Indicate whether pressure vessels are designed to ASME Pressure Vessel Code, MIL-STD-1522, DOT requirements or other design approved by OSC Safety. If fracture mechanics is used to justify lower safety factors, a description of the methodology and references for the analysis shall be provided.

k. Plans for initial pressurization. In order to Satisfy remote pressurization requirements, blast/fragment hazard of a pressure vessel rupture must be analyzed. The combination of pressure and volume in the tank corresponds to

a TNT equivalency. The blast shield/wall to be utilized must provide the proper protection for the particular pressure vessel. Besides providing fragment protection, consideration should be given to relieving the over pressure in such a way as to minimize injury to personnel and damage to facilities.

3.5 Ordnance Subsystems

3.5.1 Design Requirements

This section establishes the policies and procedures to be met in design and operations such as transporting, handling, sorting, installing, testing and connecting ordnance at the VAB.

Ordnance subsytem and component design should follow the safety requirements specified in MIL-STD-1576.

a. Ordnance is defined as all electro-explosive devices (EED's) or laser initiated detonators, squibs, primer, pyrotechnic devices, initiators, ignitors, solid propellants, explosives, warheads, ammunition, fuzes and energy transfer systems including, but not limited to, Primacord, Superzip, Mild Detonating Fuze (MDF), Confined Detonation Fuze (CDF) and Linear Shaped Charges (LSC).

b. In addition to ordnance devices, this section addresses the entire electro-explosive subsystem which for the purposes of this section is divided as follows:

   (1) Power Source: This can be a battery, on dedicated power bus .

   (2) Firing Circuit: Current path between the power source and the initiating device.

   (3) Control Circuit: Activates/deactivates the safety devices in the firing circuit.

   (4) Monitor Circuit: Verifies the status of the firing circuit. Control (i.e., command) circuits can also be monitored, however, they are not accepted as a firing circuit monitor.

   (5) Initiating Device: Converts electrical or mechanical energy into explosive energy.

c. Transportation, storage and handling requirements are applicable to all ordnance items. Only those initiating devices deemed to be a hazard are subject to the design requirements of his section. A device can be considered hazardous if it is Category A or if it is inaccessible and a hazardous operation such as vehicle disassembly would be required to replace it after an inadvertent firing. Where there is doubt as to the safety of a particular device or its usage, the design requirements of this section shall apply. A device is considered hazardous regardless of the precautions against inadvertent firing.

d. Electro-explosive devices shall be designed to include safety features and proven operational reliability to preclude inadvertent firing or degradation of any

explosive or pyrotechnic components in the ordnance system, when subjected to specific environmental conditions.

e. The requirements specified herein provide the minimum design criteria for ordnance items. Requirements are based on current design practices and are not considered a restraint on the development of new technology.

3.5.2 Hazard Classification

a. Ordnance items shall be assigned the appropriate military (DoD) hazard classification and storage compatibility group in accordance with DoD 6055.9-STD, Chapter 3. Items which have not previously been classified (and cannot be classified based on similarity with previously classified items) shall be tested IAW TB 700-2 (NAVORD Inst 8020.3) and classified accordingly.

b. All initiating ordnance items, for example, EED's, shall be classified as a category A (hazardous) or B (non-hazardous) device for both the pre-installation and post-installation situations. The VAB User is responsible for classifying each device and submitting a list with justification for the category assignment.

(1) Category "A" electro-explosive devices are those which, by the expenditure of their own energy or because they initiate a chain of events, may cause injury (or death) to people or damage to property.

(2) Category "B" devices are those which will not, in themselves (hand safe) or by initiating a chain of events, cause injury to people or damage to property.

3.5.3 Electro-explosive Devices (EEDs)

a. Ordnance items such as solid propellant rocket motors, destruct charges and other major ordnance systems shall be designed so that the sensitive initiating elements can be installed in the system just prior to electrical hookup. The ordnance locations shall be accessible to facilitate installation/removal and electrical connections as late as possible.

b. The final electrical connection of an EED to the firing circuit shall be as close to the EED as possible.

c. Design should take into account the following considerations: bonding and grounding, electromagnetic compatibility with the environment, service life 10 years), selection of fungus inert materials, selection of reactive/non-reactive materials and environmental durability. Environmental design consideration shall, as a minimum, meet the applicable criteria (shock, vibration, temperature, etc.) of MIL-STD-1540B, DOD-E-83578A or other DoD agency approved specification for ordnance devices.

d. One Amp/One Watt No-Fire Survivability is required, as determined from the 0.1% firing level of the EED (with 95% confidence) using the Bruceton test or equivalent statistical testing.

e. The no-fire current shall not be less than one ampere as the result of the application of a DC voltage for five minutes, without the use of external shunts.

f. The no-fire power shall not be less than one watt as the result of the application of a DC voltage for five minutes without the use of external shunts.

g. All Category A EED's shall be capable of withstanding a 25Kv discharge (pin-to-case and pin-to-pin) from a 500 pfd capacitor. Discharge path resistance will not exceed 5000 ohms. Mil-Std-1512 and Mil-Std-1576 describe test set-ups.

h. The EED main body shall not rupture or fragment when the device is fired. Displacement or deformation of the connector and main housing is permissible. Rupture or deformation of the outer end is permissible.

i. The insulation resistance between pin-and-case shall be greater than 2 megohm at a minimum of 500 volts DC potential.

j. The main body (outer case) shall be made from a conductive material, preferably metal.

k. The explosive or pyrotechnic mix shall not degrade, decompose or change chemically over the life of the device. Devices shall be designed for a minimum ten year shelf life. All EED's shall require re-acceptance testing after ten years from the date of manufacture. The extent of re-acceptance testing will be determined on a case-by-case basis.

l. EEDs shall not auto ignite when exposed to thermal environments that are 30 degrees C above maximum predicted temperature during worst case service life. EEDs shall not decompose when subjected to thermal environments that are 30 degrees C above the maximum predicted temperature and 10 degrees C below the minimum predicted temperature during worst case service life, if decomposition or failure to function can create a hazard. The auto ignition temperature shall not be less than 300° F.

3.5.4 Laser Initiated Ordnance

To Be Determined

3.5.4 Shielding Caps

Shielding caps shall be provided and placed on the EED during shipment, storage, handling and installation up to the point of electrical connection.

3.5.5 Shields

a. The firing circuit shall be completely shielded or shielded from the EED back to a point in the firing circuit at which filters or absorptive devices eliminate RF entry into shielded portion of the system.

b. Shielding shall provide a minimum of 85 percent of optical coverage ratio. Optical coverage is the percentage of the surface area of the cable core insulation covered by a shield. A solid shield rather than a mesh would have 100% optical coverage. (≥ 20dBA attenuation below EED no-fire levels is required)

c. There shall be no gaps or discontinuities in the shielding, including the termination at the back faces of the connectors. Connectors and containers must provide RF attenuation as not to circumvent the protection provided by the shielded cables.

d. Shields terminated at a connection shall be electrically joined with non gaps around the full 360 degree circumference of the shield.

e. All metallic parts of the electro-explosive subsystem shall be conducted with a DC impedance of less than 2.5 milli-ohms.

f. Firing circuits and control circuits, which are not activated at the same time, shall be shielded from each other.

3.5.6 Wiring

a. Twisted shielded pairs shall be used unless other configurations can be shown to be more effective, for example, coaxial leads. Splicing of wires or shields is prohibited.

b. Firing circuits and EEDs shall be isolated from the EED case and other conducting parts of the vehicle. If a circuit must be grounded, there shall be only one interconnection with other circuits (single point ground). This interconnection shall be at the power source only. Static bleed resistors of 10K ohms or more are not considered to violate the single point ground. Other ground connections with equivalent isolation shall be handled on a case-by-case basis.

c. Ungrounded circuits, capable of building up static charge, shall be connected to structure by static bleed resistors of at least 10K ohms.

d. Electro-explosive subsystem design shall preclude sneak circuits and unintentional electrical paths due to ground loops, failure of solid state switches, etc.

e. Insulation resistance between all insulated parts, at 500 volts DC minimum, shall be greater than 2 Megohms.

f. Firing circuit conductors shall be clearly and specifically discernible from other electrical circuits and identified as such. In addition, all firing circuit wires contained within junction boxes shall be physically isolated from other circuits and shall also be identified.

3.5.7 Connectors

a. The plug and socket type is preferred.

b. The outer shells shall be made of conductive metal.

c. Mating of connectors shall be controlled to significantly reduce the chance of mis-mating where catastrophic or critical hazards may occur. Positive design features, rather than procedural controls and inspection, shall be used to prevent mismating of connectors.

d. Connectors shall be of the self-locking types. Lock wiring or equivalent shall be utilized to prevent accidental or inadvertent demating.

e. The design shall ensure that the shielding connection is completed before the pin connection. This is both an electrostatic and RF protection concern.

f. The circuit assignments and isolation of pins within a connector shall be such that any single short circuit occurring as a result of a bent pin shall not results in more than 10% of the actuation current (50 milli-amps maximum) applied to any electro-explosive subsystem circuit.

g. There shall be only one wire per pin, and in no case shall a connector pin be used as a terminal or tie-point for multiple connections.

h. Spare pins are prohibited in connectors where a broken pin may have an adverse effect on a firing or control circuit.

i. Where redundant circuits are required for safety critical functions, separate connectors shall be used.

j. Source circuits shall terminate in a connector with female contacts.

3.5.8 Safety Devices

a. Safety devices are electrical, electo-mechanical or mechanical devices which are utilized in all electro-explosive subsystems to provide electrical and mechanical isolation between each initiator and the power source and the rest of the ordnance train. These devices may permit programmed checkout or

status of the firing circuits and initiators. Examples include Safe and Arm devices, Arm/Disarm devices, relays, mechanical and solid state switches, and arming/safing plugs.

b. All Category A (Catastrophic) firing circuits shall have at least three independent electrical inhibits that provide interruption of the circuit when ever ordnance is connected. Each of these inhibits shall be monitored whenever power is applied to the system and shall only be removed after the vehicle/payload have reached a safe distance from the carried aircraft .

c. All Category A (Critical) firing circuits shall have at least two independent electrical inhibits that provide interruption of the circuit when ever ordnance is connected. One of the two inhibits shall be monitored whenever power is applied to the system and shall only be removed after the vehicle/payload have reached a safe distance from the carried aircraft .

d. Destruct systems and Category A solid motor ignition circuits for the vehicle and all payloads shall include a Safe & Arm device. An S&A may be required on other systems depending on the degree of hazard. After ordnance and firing circuit connection, S&A devices may not be rotated to the Arm position until two seconds after the planned drop from the carrier vehicle. Exceptions to these requirements will be handled on a case-by-case basis and must be requested in writing.

3.5.8.1 Safe and Arm Devices

These devices provide mechanical and electrical isolation of the initiator from the primary explosive or pyrotechnic.

a. The design shall incorporate provisions to safe and arm the ordnance train from any rotor position.

b. Remote and manual safing shall be accomplished without passing through the armed position.

c. When the device is in the safe position, the power and return lines shall be disconnected, the bridgewire will be shorted and grounded through a 10K (minimum) ohm resistor and the explosive train shall be interrupted by a mechanical barrier capable of containing the initiator's output energy without initiating the primary explosive.

d. When the device is in the arm position, the short shall be removed, there shall be a mechanical alignment of the explosive train and electrical continuity from the firing circuit connector to the initiator within the device. The bleed resistor should not be removed.

e. The device shall not be capable of propagating beyond the detonators with the barrier rotated less than 50 degrees (50 percent for sliding barriers).

f. Safe and arm devices shall be capable of being remotely armed. They shall not be capable of being manually armed, but shall be capable of being manually safed.

g. A remote status indicator shall be provided to show the armed or safed condition. The device shall also indicate its arm or safe status by simple visual inspection. There shall be easy access to this visual indication throughout vehicle/payload ground processing.

h. The safe position shall not be indicated visually or remotely unless the device is less than 10 degrees from the normal safe position for rotating systems or 10 percent for sliding barriers. The arm position shall not be indicated unless the device is in a position which will align the explosive train and allow initiation with the required reliability. In between these two positions, no remote indication shall appear.

i. The electrical continuity of one status circuit (safe or arm) shall completely break prior to the time that the electrical continuity is established for the other status circuit (safe or arm) Continuity of the safe circuit shall be established immediately after the firing circuits are opened and initiators leads (S&A) are shorted. Electrical contacts shall be designated to prevent chatter, for example, use wiping tape (disc-mounted) contacts.

j. During checkout, the safe or arm status circuits shall be capable of being monitored electrically by ground support equipment , such as that provided at the ordnance storage facility and at the VAB.

k. The explosive train shall remain disconnected during prelaunch checkout (rotation).

l. The mechanical lock within the device shall prevent inadvertent arming/safing under worst case environmental conditions.

m. A positive mechanical lock and safety pin shall be used in the device to prevent movement from the safe to the arm position.

n. Rotation of more than 10 degrees shall not be possible with the safety pin installed.

o. Removal of the safety pin shall be impossible if the arming circuit is energized or if arming force is applied.

p. Removal of the safety pin shall not cause the device to arm.

q. Removal of the safety pin shall be inhibited by a suitable detent or preferable by a locking mechanism requiring 90° rotation of the pin.

r. The pin shall, through normal insertion, manually safe the device (if armed).

s. All S&A devices shall be designed to withstand repeated cycling from the arm to the safe positions for at least 1000 cycles, without any malfunction, failure or deterioration in performance.

t. A constant one hour application of arming voltage with, and without, the safe pin installed shall not cause the detonator or rotor leads (explosive mix) to fire.

3.5.8.2 Arming and Safing Plugs

These devices provide electrical isolation of the initiator from electrical power source, but cannot be armed or safed remotely.

a. Safing plugs shall be designed to electrically isolate and short the initiator side of the firing circuit. Isolation shall be a minimum of 10K ohms.

b. Arming and safing plugs shall be designed to be positively identifiable by color, shape and name.

c. The design of the device and the firing circuit shall ensure easy access for plug installation and removal during assembly and checkout.

d. Monitor and control circuits shall not be routed through safing plugs.

e. These devices shall meet the electro-explosive subsystem shielding requirements of this section.

3.5.8.3 Switches and Relays

These devices are normally contained in firing units or safety devices such as S&As and utilized independently for interruption of the firing circuit. They may be either of the electro-mechanical or solid state type.

a. Switches and relays shall be designed/selected to reliably function at expected operating voltages and current under worst case environmental conditions, to include maximum expected cycle life.

b. Relays shall be designed/selected to prevent chatter when subjected to the worst case environment.

c. Switches and relays shall not require power to perform as a safety device.

d. Arrangement of switches, relays and other safety devices shall maximize safety by placing the most positive/reliable form of circuit interruption closest to the EED, for example, locate a safe plug downstream of a solid state switch.

3.5.9 Monitoring, Checkout and Control Circuitry/Equipment

a. All circuits used to arm or disarm the firing circuit shall contain a means to provide remote electrical indication of their armed or safe status.

(1) Category A (Catastrophic) firing circuits shall have at least three independent electrical inhibits that provide interruption of the circuit when ever ordnance is connected. Each of these inhibits shall be monitored whenever power is applied to the system and shall only be removed after the vehicle/payload have reached a safe distance from the carried aircraft .

(2) All Category A (critical) firing circuits shall have at least two independent electrical inhibits that provide interruption of the circuit when ever ordnance is connected. One of the two inhibits shall be monitored whenever power is applied to the system and shall only be removed after the vehicle/payload have reached a safe distance from the carried aircraft .

b. These circuits shall be completely independent of the firing circuits and shall use a separate and non-interchangeable electrical connector.

c. Circuits to monitor other critical parameters such as firing circuit continuity, resistance and stray voltage are optional as part of the flight system or its GSE.

d. Monitoring, checkout and control current shall not exceed one-tenth the no-fire current of the EED, or 100 mA, whichever is less. Circuits shall be designed such that application of operational voltage will not compromise the safety of the firing circuit nor cause the electro-explosive subsystem to be armed.

e. No single point failure in monitoring, checkout or control circuitry/ equipment shall compromise the safety of the firing circuit. Consideration should be given to the design, construction and operation of the circuitry/equipment.

3.5.10 Ordnance Test Requirements

The requirements specified herein provide the minimum test criteria for ordnance items, circuits and associated devices.

a. QUALIFICATIONS AND ACCEPTANCE TESTS - All EEDs, explosive subsystems and components shall be tested to ensure they reliably meet the requirements of this manual when subjected to the static, dynamic and electromagnetic environments of the launch vehicle, payload, facility and GSE during transportation, handling, assembly and checkout. Reliability testing for EEDs can be accomplished using the Bruceton Method or other equivalent statistical technique. Guidance on EED and S&A testing can be found in MIL-STD-1540B, DOD-E-83578A , Mil Std 1512 and Mil Std 1576.

b. EED CATEGORIZATION - Testing to determine EED hazard category (A or B) shall provide the following:

(1) Handheld Mode. Function at least 1% of an EED lot or at least 10 units to determine if the EED produces fragments, temperature rise above 500°F, produces flame or produces pressure in excess of 500 psig at the output end. If one or more tested units produce fragments or violate the other criteria, the EEDs shall be considered category A in the handheld mode.

(2) Assembled Mode. Perform an analysis of the system ordnance train or function of the EED to determine if its initiation is capable of causing injury through a chain of events associated with the subsystem or system, for example, motor ignition, boom release, etc. Tests will not normally be required for the assembled mode.

(3) Analysis vs Test. It is not the intention of this document to impose excessive test requirements. Similarities with previously tested items is often sufficient for categorization. If testing or analogy is not accomplished, the EED shall be treated as Category A.

c. HAZARD CLASSIFICATION - All ordnance items used at the VAB shall be tested to determine the appropriate military hazard classification IAW DOD 60559. The tests shall be IAW procedures prescribed by AFTO 11A-1-47, NAVSEA INST 8020.8. Items of similar chemical composition to items already tested and classified may not require additional testing.

d. TEST EQUIPMENT - All ordnance test equipment such as continuity and bridgewire resistance checkers shall be inspected and tested for voltage isolation and limitation at a Certified Calibration Laboratory.

3.5.11 Ordnance Data Requirements

a. GENERAL - The following information is required for each piece of ordnance.

(1) Military Hazard Classification (Class, Division and Compatibility Group per DOD 5154.4S).

(2) DOT Classification (A, B or C).

(3) Manufacturer and Part Number. Include contractor part number if different from manufacturer.

(4) Chemical Composition and Characteristics, specify net explosive weight and describe all inert components, particularly the outer shell.

(5) Physical location (provide sketch) with a description of its function and the hazards associated with inadvertent functioning.

(6) Mechanical Drawings (Manufacturer's specification sheet drawings will normally suffice).

(7) Drawings (with narrative) showing location of access ports through which shorting and physical removal of each ordnance item can be accomplished including type, size and quantity of hardware involved in gaining access.

(8) Facility in which the ordnance item shall be installed, for example, factory, booster/payload buildup area, etc. Specify when the item shall be installed with respect to launch day (L-O), approximately.

(9) Specify when the item shall be electrically connected with respect to L-O day, approximately.

b. EEDs - In addition to the information above, the following information shall be provided for all EEDs. (NOTE: Similar data on Non-Explosive Initiators shall be provided as required.)

(1) Category (A or B) for pre and post installation situations .

(2) Maximum no-fire current (.995 reliability at 95% confidence).

(3) Maximum no-fire power (.995 reliability at 95% confidence).

(4) Minimum all-fire power (.995 reliability at 95% confidence, .999 at 95% for destruct systems).

(5) Bridgewire resistance and tolerance.

(6) Insulation Resistance (pin-to-case) at 500 volts, minimum.

(7) Electrostatic Sensitivity Test Values: Voltage, Capacitance, Series Resistance and modes (pin-to-case and pin-to-pin).

(8) RF Impedance (If manufacturer has this data available).

(9) RF Sensitivity (If manufacturer has this data available). If data is not available, provide an assessment of the RF sensitivity of the device by analysis/comparison or testing. OSC Safety will determine the extent of any additional testing that may be required.

(10) Qualification Test Program (Manufacturer should be able to provide a copy of their qualification test program which includes test methods, quantity tested and acceptance criteria. Test methods, which vary from MIL-STD-1512, MIL-STD 1576 or Mil-I-23659, should be described in detail).

c. CIRCUITS - The following information shall be provided:

(1) Simplified and actual schematics of the firing circuits, control circuits and monitor circuits.

(2) A narrative which explains the sequence of events which leads to the activation of the ordnance. Discuss the independence and safety features of commands and controls. Provide a time line for the planned removal of safety devices (inhibits) from the circuit.

(3) Drawings or sketches showing location of all firing circuitry/cabling, connectors, safety devices and initiators. This includes monitoring and control circuitry. Shielded circuits shall be identified.

(4) Insulation resistance at 500 volts DC between conductors.

(5) EMI Protection. Identify optical coverage of shields, the termination points of the shielding, the use of RF attenuating devices and EMC testing/analysis. Discussions shall identify the EM environment of the launch vehicle and payload.

d. MONITORING/CHECKOUT/CONTROL EQUIPMENT/CIRCUITRY: The following information shall be provided:

(1) A listing of all monitoring/checkout/control requirements as criteria.

(2) Description of all flight hardware monitoring/checkout/control circuitry. Include location sketch and electrical drawings. Specify current in this circuitry. Identify hazardous failure modes.

(3) Description and specifications sheet on ground support equipment used in monitoring/checkout/control. Specify applied current. Specify model number and calibration frequency on equipment. (Calibration seals are required). Identify hazardous failure modes.

3.6 Electrical/Electronic Equipment

3.6.1 Grounding, Bonding and Shielding

a. Equipment shall be designed/constructed to ensure that all external parts, shields and surfaces, exclusive of radiating antennas and transmission line terminals, are at ground potential.

b. In no case shall a shield be depended upon as a current carrying ground connection, except for coaxial cables.

c. Circuits which operate hazardous functions shall be adequately protected from the electromagnetic environment to preclude inadvertent operation. For guidance on electromagnetic interference protection for electronic equipment, see Mil-Std-461.

3.6.2 Connectors

a. Connectors shall have alignment pins, key way arrangements or other means to make it impossible to incorrectly mate any connector, if a hazardous condition can be created by mis-mating or reverse polarity.

b. Color coding may be used in addition to, but not in lieu of, the more positive means of mismate prevention.

c. If a hazardous event can occur, the following precautions shall be taken: Avoid the termination of power and signal leads on adjacent pins of a connector where possible. Isolate the wiring so that a single short circuit occurring in a connector cannot affect other components. Avoid the possibility of an inadvertent pin-to-pin short. Arrange termination to minimize the potential short circuit hazard. Spare pins are not allowed in connectors controlling hazardous operations or OSC Safety critical functions.

d. The elements of a redundant circuit shall not be terminated in a single connector where the loss of such connector will negate the redundant feature. Redundant circuits should be separated to the maximum extend possible. Redundant circuits are required if loss of power or signal may result in injury to personnel or detriment to a safety critical system.

e. Uninterrupted wires are preferred over connectors, particularly if a safety critical system is involved. If connectors are required for a safety critical flight system, they shall be of the locking type or have other means of positive control such as sealing with epoxy.

f. Male connectors shall not be capable of being energized i disconnected from the female connector.

g. Connectors relying on spring contact shall not be used. Plug and socket type connectors shall be used, where possible.

3.6.3 Cables

a. Cables shall be given proper support and protection against abrasion or crimping. Cables shall be located or protected as not to present a tripping hazard, where feasible.

b. Cables shall be selected with the following criteria in mind: insulation resistance, shielding, toxicity, combustibility/smoke production, off gassing, etc.

3.6.4 Batteries

a. Batteries shall be capable of being easily disconnected and removed unless a risk assessment can demonstrate that all potential hazards are adequately controlled. Batteries must be removed or configured in a safe condition during propellant transfer operations

b. Polarity of terminals shall be marked

c. Connections shall be designed to prevent reverse polarity.

d. Sufficient ventilation shall be provided.

e. Battery charging current shall be limited by design. Battery charge current shall not be able to initiate or sustain a run-away failure of the battery. Two fault tolerance is required to prevent a thermal run-away condition of the battery which could lead to catastrophic hazard.

f. Batteries should be sealed. Sealed batteries shall have pressure relief capability, unless the cell has a 4:1 safety factor with respect to worse case pressure build-up, without failure. Vented batteries shall vent gases to an area where ignition of gas is impossible.

g. Battery cells which recombine hydrogen and hydroxide shall be used where practical.

3.6.5 Electrical/Electronic Data Requirements

a. Provide a brief description of the power sources and the power distribution network.

b. Describe how faults in electrical circuitry are prevented from propagating into hazardous subsystems. Included in this discussion would be dedicated power sources/buses, use of fuses, wiring sizing, etc.

c. Describe how inadvertent commands are prevented, for example, software safety and critical commands listing. (NOTE: This is sometimes discussed in the non-ionizing (RF) radiation (Tracking, Telemetry and Command) section of a SDP/ARAR.)

d. Identify potential shock hazards.

e. The following data shall be provided for all batteries.

(1) Design versus actual operating parameters of cells and battery. Specify the system which uses the battery.

(2) Cell chemistry and physical construction.

(3) Cell vent parameters.

(4) Toxic chemical emission of cells and evaluation of hazards.

(5) EPA classification of battery.

(6) DOT classification of battery.

(7) Physical and electrical integration of cells to form the battery.

(8) Description of safety devices.

(9) Test results.

(10) Case design including vent operation and battery case housing yield point.

3.7 Non-Ionizing Radiation

3.7.1 RF Emitter Design Requirements

a. RF equipment shall be designed and located to allow test and checkout without presenting a hazard to personnel, ordnance or other electronic equipment.

b. Personnel shall not be exposed to RF levels in excess of those specified in AFOSH Std 161-9, "Exposure to Radio frequency Radiation." Antenna hats shall be utilized to minimize exposure to personnel during ground checkout unless an analysis of the RF hazard are is performed.

c. Electroexplosive subsystems shall not be exposed to RF radiation which is capable of firing the electroexplosive device by pin-to-pin bridgewire heating or pin-to-case arcing. Electroexplosive subsystems which meet the requirements of this chapter and are processed in approved ordnance facilities will not normally require any analysis. The siting of RF emitters in proximity to electroexplosive subsystems shall be in accordance with the tables provided in AFR 127-100.

d. Local RF silence (launch vehicle and mobile transmitters) is required during periods of ordnance (EED) installation, removal and electrical connection/disconnection aboard a vehicle/payload. RF and ordnance systems shall be designed to avoid any conflict as the result of this policy.

e. Interlocks, interrupts or other safety devices shall be provided where necessary to protect operating personnel during ground operations.

3.7.2 RF Emitter Test Requirements

a. The VAB users shall have the RF hazard area verified by a designated representative prior to first operation/test.

b. All VAB should perform RF measurements on their systems to verify hazard areas except for those low power systems deemed a negligible radiation hazard.

3.7.3 RF Emitter Data Requirements

a. The following data is required for RF equipment.

(1) Transmitter peak power and average power.

(2) Pulse widths.

(3) Pulse repetition frequencies.

(4) Pulse codes.

(5) Maximum rated duty cycle.

(6) Type and size of antenna.

(7) Antenna gain and illumination.

(8) Beam width and beam skew.

(9) Operating Frequency (MHz).

(10) Insertion loss between transmitter and antenna.

(11) Polarization of transmitted wave.

b. An analysis of the RF hazard area with and without antenna hats/dummy load, and results of any testing. A table which lists all of the RF emitters aboard a vehicle and their hazard areas (distances) shall be provided.

3.8 Acoustic (Noise) Criteria

Personnel shall not be exposed to hazardous noise levels. The OSC Safety Engineer is responsible for evaluating noise levels and determining the hazard potential. Methods of protection for personnel who may be exposed to sound pressure levels above 85 dBA shall be identified.

Appendix A
Accident Risk Assessment Report/
Safety Data Package
Recommended Format

- INTRODUCTION
  - Purpose
  - Scope
  - Safety Certification
  - Program Safety Status Summary
  - Non-Compliant Items
  - Vehicle Description
- DETAILED SYSTEM DESCRIPTIONS
  - Structural/Mechanical Subsystems
  - Propulsion/Liquid Propellant Subsystems
  - Pressurized Subsystems
  - Ordnance Subsystems
  - Electrical/Electronic Subsystems
  - Non-Ionizing Radiation - RF and Command Subsystems
  - Ionizing Radiation Producing Subsystems
- GROUND OPERATIONS
  - Structural/Mechanical
  - Propulsion/Liquid Propellant
  - Pressurization
  - Ordnance
  - Electrical/Electronic
  - Non-Ionizing Radiation
  - Ionizing Radiation
  - Noise Protection
- HAZARDOUS MATERIALS
- PERSONNEL PROTECTIVE EQUIPMENT
- HAZARD ANALYSES/HAZARD REPORTS
- HAZARDOUS PROCEDURES
- FAILURE/ACCIDENT RECORD